Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут ім. Ігоря Сікорського”

Фізико-технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

з предмету «Криптографія»

«Криптоаналіз шифру Віженера»

Виконав:

Студент 3 курсу,

ФТІ, групи ФБ-05

Савченко Ярослав

Київ - 2022

**Мета роботи**

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу

потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

**Порядок виконання роботи**

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3,4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

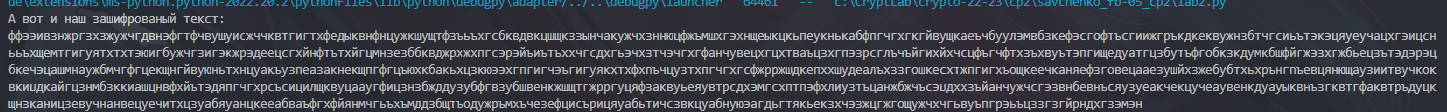
**Варіант №9**

**Хід роботи**

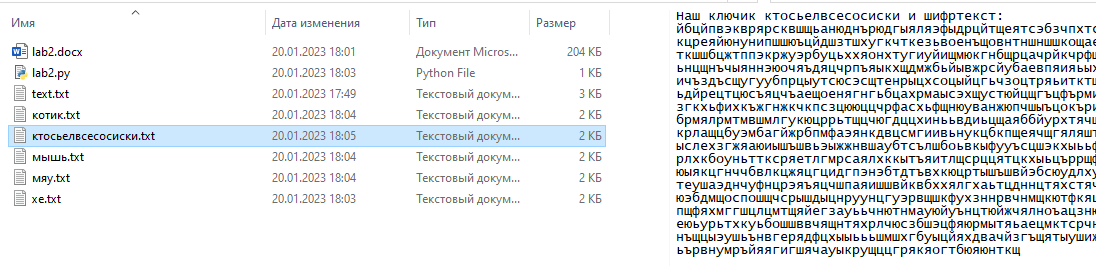
Оберемо фрагмент з тексту на 2кб, що використовували в першій лабораторній.

Напишемо код, що буде шифрувати наш текст. Візьмемо декілька рядків з коду першої лабораторної роботи для роботи з файлами.

Для зручності зробимо так, щоб ми могли вказувати ключ зашифрування безпосередньо перед зашифруванням прямо в консолі.

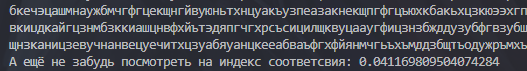


Чудово, все працює. Зробимо це для всіх наших ключів



Також зробив запис зашифрованого тексту у файл з назвою ключа для зручності :3

Тепер для наступної задачі додамо функцію для знаходження індексу відповідності. Його також запишемо в файл



Чудово :3

Порахували для кожного і побудували діаграму



Зовсім трохи, але можемо побачити що індекс зменшується з довжиною ключа. Якби ми взяли більше ключів, то побачили б спадний графік ще краще.

А також я пропустив прорахування для відкритого тексту, але швидко це виправив

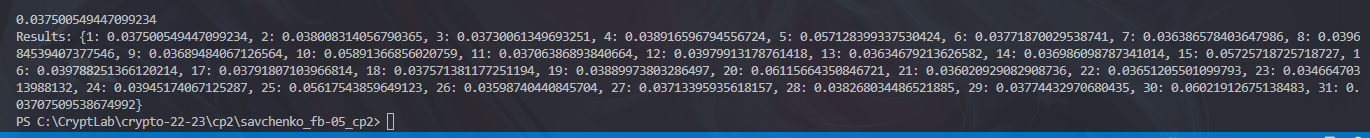




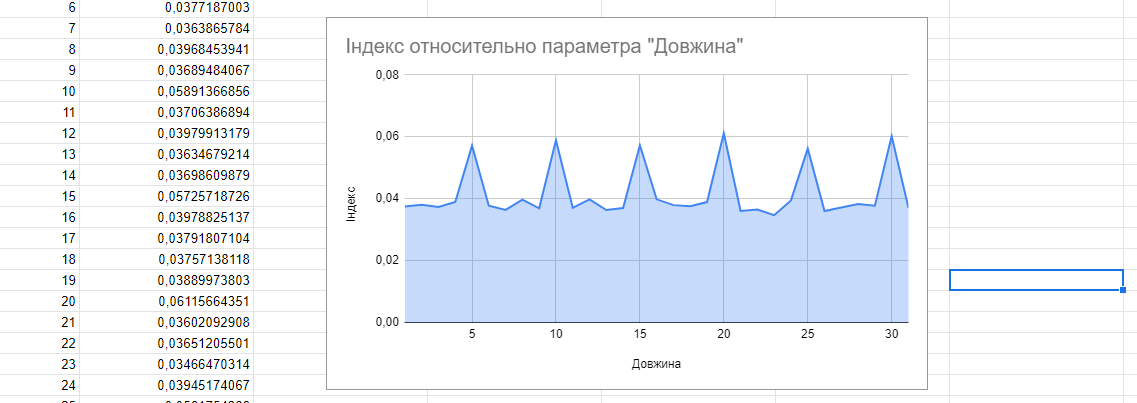
Перейдемо до найцікавішого. Розшифрування тексту за варіантом.

Збережу текст свого варіанту в файл, та створю окремий python файл для цього завдання.

Спочатку напишу функцію що порахує індекс відповідності для всіх можливих довжин ключа до 32

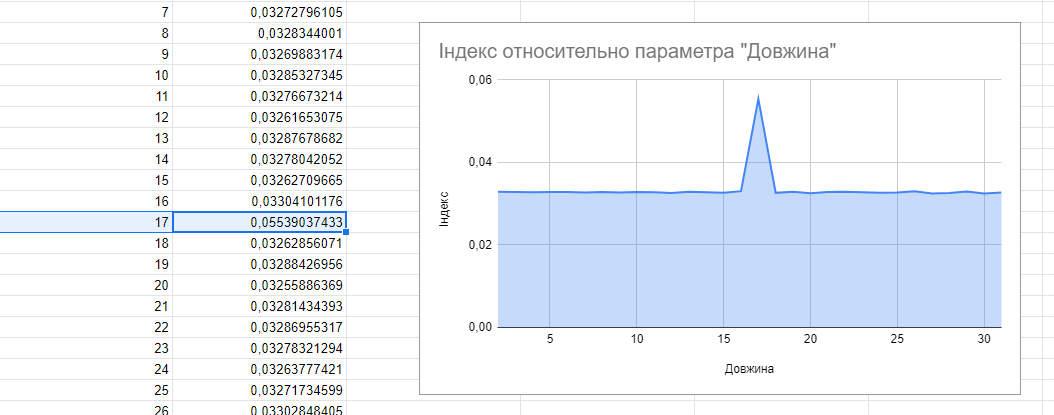


Тут ми бачимо що індекс досягає найбільшого значення кожні 5 довжин. Для зручності перенесу дані в таблицю і покажу графік



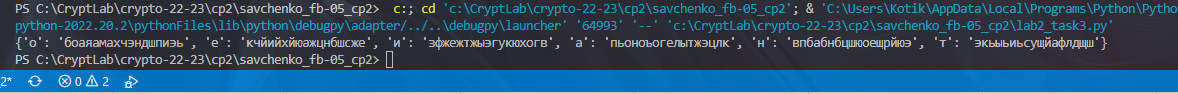
Тепер знаючи довжину ключа знайдемо його. Для цього створимо нову функцію що за довжиною ключа та даними з першої лабораторної роботи видасть результати

На цьому моменті я отримав бурю емоцій адже зрозумів що весь цей час намагався знайти ключ довжини 5... Але ця довжина ключа була знайдена для одного з моїх файлів. Витративши більше 6 годин щоб це зрозуміти я врешті решт виконав частотний аналіз для потрібного шифтексту (нарешті) і отримав результат з яким працював далі

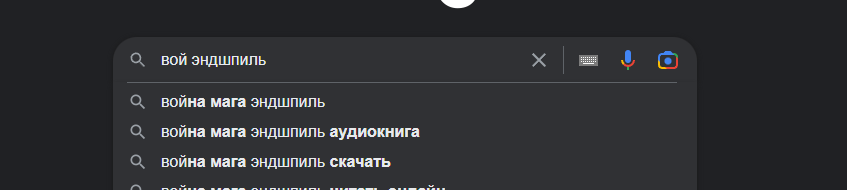


Тож довжина зашифрованого тексту – 17

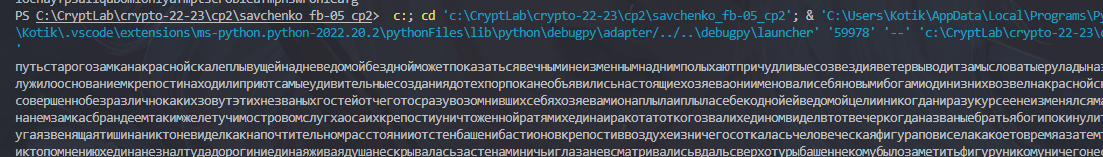
Напишемо функцію для знаходження можливого схожого ключа користуючись методом з методички і знайдемо результат



Ммда... Не густо. Але в очі кинулося можливе слово “эншпиль”. Почав копати під нього)

Взявши можливі слова та просто перші можливі букви та повводивши все в гуглі наткнувся на такий запрос

Роман письменника Ніка Перумова. Використаємо його як ключ для розшифровки. Допишемо функцію розшифрування і отримаємо початковий текст



“Путь старого замка на красной скале плывущей над неведомой бездной может...”

Висновок: на цій лабораторній роботі я навчився навичкам частотного криптоаналізу. Принципам шифрування, методам знаходження довжини ключа та значення самого ключа. А також навчився бути уважнішим до свого ж коду, в якому встиг не раз запутатися через один єдиний параметр :)